Before the

Federal Communications Commission

Washington, D.C. 20554

In the Matter of	)	
	)	GN Docket Nos. 09-47, 09-51, 09-137
Additional Comment Sought on Public Safety,	)	PS Docket Nos. 06-229, 07-100, 07-114
Homeland Security, and Cybersecurity Elements	)	WT Docket No. 06-150
of National Broadband Plan	)	CC Docket No. 94-102
	)	WC Docket No. 05-196
NBP Public Notice #8	)	

Comments

The State of New York ("the State") hereby submits comments in response to the Federal Communication Commission's ("Commission") National Broadband Plan public notice #8 dated September 28, 2009.

Response to 1. Public Safety Mobile Wireless Broadband Networks.

Currently in New York State there is varied use of commercial broadband wireless services by public safety agencies at the local and state level. Also, there is significant interest in deploying a broadband network across New York for exclusive public safety use at the local and state level.

Recently, the New York State Association of Counties (NYSAC) in partnership with the State submitted an innovative proposal for American Recovery and Reinvestment Act (ARRA) funding administered by the National Telecommunication and Information Administration (NTIA) and the Rural Utility Services (RUS). The purpose of this proposal is to build a fourth generation (4G) 700 MHz broadband network for public safety use in thirty-six (36) participating rural and non-rural counties across New York.

Central to the proposed solution is inter-county roaming support so that authorized public safety users can successfully roam the network within any county participating in the deployment. This project will utilize the emerging Long Term Evolution (LTE) technology standard for the mobile terrestrial network infrastructure. The Association of Public Safety Communication Officials (APCO), the National Public Safety Telecommunications Council (NPSTC), and the Public Safety Spectrum Trust (PSST) have endorsed LTE as the preferred technology standard for mobile broadband services for public safety. Additionally, several of the larger network providers of commercial mobile broadband services have indicated LTE will be used in the construction of their 4th Generation (4G) commercial networks.

The network will support a variety of applications which public safety users can access during normal and emergency field operations. Applications include streaming video (surveillance, remote monitoring), digital imaging, automatic vehicle location, computer aided dispatching, e-mail, mapping/GIS, remote database access, report management system access, text messaging, telemetry/remote diagnostics, and web access, both Intranet and Internet. When fully deployed it is anticipated that approximately 90,000 public safety users across the participating counties will use the system.

Initially, the majority of users will access the proposed broadband network using laptops with air interface cards. Other devices, perhaps with smaller footprints, may become available as new products are introduced by a variety of companies.

Where possible, the proposed network will use existing communications infrastructure across the State. Many participating counties already have in place extensive land mobile radio (LMR) systems. While the proposed broadband network is not considered as a replacement to these LMR systems, efforts will be made to share infrastructure when possible and for cost savings. In particular, opportunities may exist to utilize existing microwave and wired backhaul networks at the county and state level to also serve the broadband network.

The proposed public safety broadband network will have stringent network reliability and availability requirements, which may be higher than requirements typically associated with commercial networks. These requirements will require extensive component redundancy of key network components to minimize potential downtime. Redundant routers, switches, and base station components are typical requirements needed for public safety networks.

New York's strategy recognizes that under some conditions it is more cost effective and beneficial to have public safety resources utilize commercial broadband networks. Given New York's commitment to building a public safety LTE broadband network, commercial 4G LTE 700 MHz solutions planned for implementation within the state are especially appealing from an integration perspective. This approach provides the best chance to provide public safety users with a wireless broadband infrastructure which allows seamless, uninterrupted roaming between networks as one traverses the state.

New York encourages the Commission to adopt strategies that promote technology standards, but at the same time create and maintain competition in the marketplace. Cost effective solutions with product choice are the optimal conditions for expanding public safety broadband networks in a budget-constrained environment. Technology standards discourage proprietary solutions and encourage competitive pricing as product manufacturers have access to expanding markets. Additionally, technology standards which are also adopted and utilized in the commercial sector provide the right economic conditions for lower priced products and components.

Response to 3. Cyber Security

a. What type of computer-based attacks against government or commercial computer systems or networks (i.e. cyber attacks) are occurring or are anticipated to occur, and what are other federal agencies, commercial, and other entities doing to prevent, detect and respond to cyber attacks?

The types of attacks range from very sophisticated, targeted attacks from organized crime or nation states to unsophisticated "script kiddie" attacks. For public broadband, the nature of these attacks is not expected to change. However, mobile wireless broadband service provides new threat opportunities. The devices required for these services do not provide the customary layered defenses such as firewalls, antivirus software, authentication, encryption, etc. As adoption of mobile wireless broadband service increases, it provides an opportunity for a new and expansive threat which can then be used to infiltrate existing networks. One possible scenario would include connecting a compromised mobile device to a network so that it would compromise other devices. To respond to these attacks, organizations are implementing layers of security so that if one layer is breached, another layer will detect or limit the scope of the breach. Updating software, keeping abreast of the threat landscape as well as conducting security awareness training for staff are critical components of an organization's security posture. Vulnerability and application testing, penetration tests and security assessments are instrumental in insuring that security controls are in place and functioning properly. Additionally, sharing and collaborating about new threats, vulnerabilities, attacks and protection mechanisms through Information Sharing and Analysis Centers (ISAC's) across the entire industry is an important vehicle for situational awareness.

b. How are other federal agencies of the United States and other governments collaborating with the communications segment to prevent, detect, and respond to cyber attacks?

In New York State, the Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) has established a public/private partnership with most of the critical infrastructure sectors including the communications industry. Monthly conference calls are held with NYS telecommunication providers. This creates a forum for trusted relationships and the exchange of information. In addition, CSCIC is the coordinator of the Multi-State Information Sharing and Analysis Center and there is an informational exchange with the other ISAC's and the Federal Government with respect to threats, vulnerabilities, attacks, and protection mechanisms.

c. What market incentives exist for commercial communications providers, large and small, to invest in secure infrastructure? (i.e., how do we avoid externalities?)

We are not familiar with any market incentives that may exist.

d. Do end-users have sufficient independent information to make good decisions between communications providers that may differ in the extent to which they implement cyber security measures?

In general, end users lack the knowledge, understanding, and experience to evaluate the differences among various communication providers and the cyber security measures they offer. Evidence of this lack of end user sophistication is found in the fact that some 6 million computers are still infected by the Conficker worm a year after it initially emerged. Many of these infected machines have IP addresses belonging to broadband users, many of whom would be assumed to be home users.

e. How widely are cyber security best practices implemented by communications providers and what are these best practices?

We are unfamiliar with cyber security best practices implemented by communications providers. However, if, at a minimum, communications providers could provide a "walled garden" or quarantine area for any computers on their network which exhibit symptoms of infection, this would be a significant improvement in combating botnets and propagation of other malicious software.

f. What are the specific wireless network features and handset features and capabilities necessary to combat such attacks?

Wireless network features and handset features need to implement many of the same features that we find in a wired network such as anti-virus, anti-spam, firewall features including "walled gardens," and quarantine areas for infected machines. End point protection is essential to thwart evolving viruses, worms, and other malicious software threats. Authentication and encryption is a requirement since the "Microsoft Security Intelligence Report", Volume 7 covering the period January through June 2009 indicates four-fifths of all breaches are as a result of lost or stolen devices. Encrypted handsets minimize exposure of sensitive data when handsets are lost. A "find me" feature using built in GPS and triangulation for lost devices and a "wipe clean" feature for unrecovered devices will also aid in mitigating exposure of sensitive data. In addition, authentication and confirmation for pairing of Bluetooth devices would aid in the effort to prevent unauthorized access. Overall, a "trustworthy computing" and security architecture needs to be implemented by design and not as an afterthought by the industry as wireless broadband expands to mobile handsets to protect the end-user and the information stored on the device.

Respectfully submitted,

Catherine H. Durand

Catherine Durand
New York State Deputy Chief Information Officer
New York State Chief Information Officer/
Office for Technology
Empire State Plaza
P.O. Box 2062
Albany, NY 12220

Thomas D. Smith

Thomas D. Smith
Assistant Deputy Director and Counsel, New York
State Office of Cyber Security
& Critical Infrastructure Coordination
30 S. Pearl Street
Albany, New York 12207-3425

November 12, 2009